Design of a new lightweight Security algorithm for Cyber Physical System to improve cyber security

Mr. P Salman Raju, Research Scholar Dept of CSE, AKNU- Rajahmundry-India, polavarapu3@gmail.com

Dr. P Venkateswara Rao, Associate Professor Dept of CSE, AKNU- Rajahmundry-India, venkat.aknu@gmail.com

Prof. SS Murthy, Director IPE-Hyderabad-India, ssmurthy@ipeindia.org

Abstract—Cyber Physical systems (CPS) are ubiquitous concept in which objects are connected to the internet and equipped with ability to sense and transmit data over a network. Consider a smart home application that makes use of CPS devices. The Internet of Things (IoT) has grown in popularity in recent years as a result of its numerous advantages, including time savings, low cost, increased human comfort, and efficient use of electricity. In smart home environments, there are various low-capacity devices (microcontrollers and sensors) connected through wireless networks. The smart devices (SDs) in the network must communicate with adequate security. Due to resource constraints like low processing power and low space, there is a lack of standard security mechanism which can provide adequate security. This research work introduces a novel key establishment mechanism with a lightweight Security algorithm for smart home systems. Proposed mechanism provides solution against various cyber-attacks like replay, masquerade, denial of service, eavesdropping etc. We demonstrate the feasibility of proposed mechanism using proof of concept and evaluate results for showing the efficiency and effectiveness of the proposed mechanism.

***Keywords*—Smart Home Networks, Network Security, Internet of Things, Cyber Physical systems, lightweight security.**

I. INTRODUCTION

Cyber Physical systems CPS is an active system that transforms a physical system into a computerized system through the use of technology and a set of instructions that govern how the system operates. CPS opportunities abound in the global market, as all major nations work on IoT-based projects to improve people's lives and enhance their quality of life. Because of CPS, even the most basic of equipment can function as a smart device. Nowadays, along with the advancement in the field of information technology, communication and electronics, there is a tremendous increase in the use and development of a smart home system (SHS). A smart home refers to a convenient home setup where appliances and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device. Devices in a smart home are interconnected through the internet, allowing the user to control functions such as security access to the home, temperature, lighting, and a home theater remotely.

SHSs exhibit various types of advance intelligence, leading to home automation systems, increasing comfort, reduction in operational costs and enhanced safety. There is an enormous business and research potential in smart appliances of smart home environments for elderly people, providing them an independent life. SHEs can also be used to provide help remotely in case of any emergencies. Recently there are a lot of research projects initiated for developing smart homes example SM4ALL (Smart Home for all) [2], HOPE (smart home for elderly people) [1], etc.

In a smart home application, there are heterogeneous smart devices like sensors, actuators, smart lights, smart windows, smart speakers, thermostats, doorbells, or home hubs, smart lights, smart fans and many other types of devices as shown in fig. 1. By bringing together a variety of heterogeneous and technical components from various sources, CPS applications connect the physical and virtual worlds. As a result, more research is needed to develop heterogeneous devices that can communicate with one another seamlessly.

The devices in a smart home like sensors, actuators etc. are low on resources like computation, memory, bandwidth and battery power. Additionally, the smart home devices communicate over an unsecured wireless channel. The smart home devices communicate with the home gateway via. a wireless channel. The home gate- way in turn may be connected to the internet. Thus, home gateway here acts like

 DOI : 10.35291/2454-9150.2022.0468

a bridge between users and smart devices. Thus, the smart home networks are widely used, allowing the users to control their household equipment's using their smart phones, tablets, web apps etc. anywhere and anytime [9][13][17].

A. *Observations*

Existing research efforts addresses CPS security related challenges and issues. While the smart home offers convenience and cost savings, there are still challenges. The research work focusing on the challenges related to cyber physical system. Security is a measure concern for current CPS based application [23]. Security risks and bugs continue to plague makers and users of the technology. Adept hackers, for example, can gain access to a smart home's internet-enabled appliances. In October 2016, a botnet called Mirai infiltrated interconnected devices of DVRs, cameras, and routers to bring down a host of major websites through a denial-of-service attack, also known as a DDoS attack. Measures to mitigate the risks of such cyber-attacks include protecting smart appliances and devices with a strong password, using encryption when available, and only connecting trusted devices to one's network.

May require additional work for homeowner to track additional passwords and monitor product security Certain required security mechanisms cannot be equipped with smart device because of space and computation requirements of those algorithms. For example, a smart device may follow the commands provided by its controller without verifying its authenticity. Thus, the resource constrained nature of these smart devices makes it difficult to provide robust security. In the recent era, a lot of work is guided towards smart home security, [13] [4] [6] [16] [22] [11] [8] most of the approaches incurred a high amount of overhead for performing device authentication while concentrating less on other security properties. The research work [19][7][18] provide insights on various security techniques and approaches based on behavior model. As per the studies, some severe threats like eavesdropping are not considered as a part of the threat model. However, in order to secure the smart devices from revealing their private data to the adversaries over an unsecured channel, there is a high requirement for the security mechanisms in smart home devices from the time they are deployed which ensures that the entities involved in the communication are authentic and not fake from the adversaries. Our proposed scheme uses symmetric key cryptography and hash functions for providing robust security in SHS. A proof of concept is provided for ensuring that the security mechanisms are robust against certain popular attacks.

A. *Contributions*

This paper makes the following contributions:

1) Study the current research trends in Security for smart home networks and identify weaknesses in existing solutions.
2) Proposes a novel secure and lightweight session key establishment algorithm.
3) Presents a proof of concept for the solution and compare it with existing solutions.

The rest of this paper is organized as follows. Section II discusses the related works, Section III illustrates the system design, section IV shows proposed scheme, section V discusses evaluation and section VI concludes the paper.

II. LITERATURE SURVEY

There are a lot of work incorporating security features for SHE. In this paper we have shown recently proposed works for SHEs.

Nikos et al. [14] presented a survey on issues, challenges and countermeasures for smart home and smart grid security. The detected threats are categorized on the basis of security goals and their impact on the overall system. Not much details are provided on how to efficiently secure against various threats after detection.

Kumar et al. [15] proposed a secure, lightweight session key establishment scheme for smart home environments which comprise of resource constrained smart devices. The proposed scheme provides prevention against various popular attacks and provides a proof-of-concept evaluation. The proposed scheme uses timestamp synchronization between heterogeneous devices which is difficult to achieve because of different clock speeds of smart devices.

Gomez et al. [9] presented various wireless home automation networks inclusive of security obstacles in INSTEON, Zigbee and Zwave, for IP based technologies. Ayday Rajagopal [3] also noticed that security support provided by Z-wave, Zigbee and INSTEON is only up to a certain level. Various secure device authentication mechanisms for smart home area networks were presented by authors. The scheme presented depends on a third party for security.

Vaida et al. [22] proposed a smart energy Home Area Network (HAN) for device authentication. The mechanism is based on elliptic curve cryptography (ECC). It establishes a session key between two involved entities. Not much details were provided for how their security mechanism is efficient and secure.

Han et al. [11] discussed a secure key pairing protocol for consumer electronics (RF4CE) for radio frequency. In this scheme, the smart devices send authentication information to mobile operator (MO) for authentication. Presented scheme is based on symmetric key

 DOI : 10.35291/2454-9150.2022.0468

cryptography. This scheme required the manufacturers to be online, which might be infeasible in certain cases.

Guillet et al. [10] introduced a novel security approach for disabled people. The scheme illustrated the discrete controller synthesis (DCS) technique to auto- mate the control of devices. The technique uses Boolean expressions for controlling device states, but Boolean expression's authenticity is not verified, thus under active attacks the scheme might not work.

Kim et al. [13] discussed an approach to integrate heterogeneous devices along with access control in smart homes. The authors observed lack of interoperable inter-device communication. Therefore, on the basis of open services gateway initiative (OSGi), they proposed a heterogeneous protocol for smart homes. In this model, only restful web API's provides remote access. A proposed scheme lacks proper device authentication for request by different users.

Lis [16] proposed a secure key establishment protocol for smart home networks. In this scheme, authors have two entities, a node and a manager are defined. Each node obtains private and public keys using a certificate authority. Security analysis provided is not in detail. On the other hand, public key operation becomes too expensive for resource limited devices.

Yosef Ashibani et al. [24] provides a security analysis of the different layers of CPS design, risk evaluation, and CPS security mechanisms. Finally, the challenges, areas for future research, and potential solutions are discussed and presented. The concepts CPS and Internet of Things (IoT) have been used interchangeably due to the large grey area of overlap. According to the author, academic institutions prefer CPS, whereas government entities and industry favour IoT.

Jacob Wurm et al. [25] looks into the security flaws of current cyber-physical systems. The analysis will span multiple layers, from Cyber-physical systems to different hardware platforms. Manufacturers can also use security solutions to help them implement security countermeasures into cyber-physical systems.

Nam Yong Kim et al. [26] mentioned that only a small amount of research has been performed in the field of CPS security because it is a new area that differs from the existing network environment. Sensors, data, real-time data obtained, performance evaluation, and application interactions are all transmitted via the CPS. The author classifies threats, strategies, and CPS security projects, and then presents solutions for each threat.

Thus, the literature survey shows us that there is a high requirement of a lightweight security mechanism for SHS from beginning of deployments of smart home networks.

III. SYSTEM DESIGN AND SECURITY PROPERTIES

A. System Design

We will consider a SHS with N number of heterogeneous smart devices like temperature sensor, smart lights, gateway server etc. The communication in between smart devices and gateway server through CPS application.

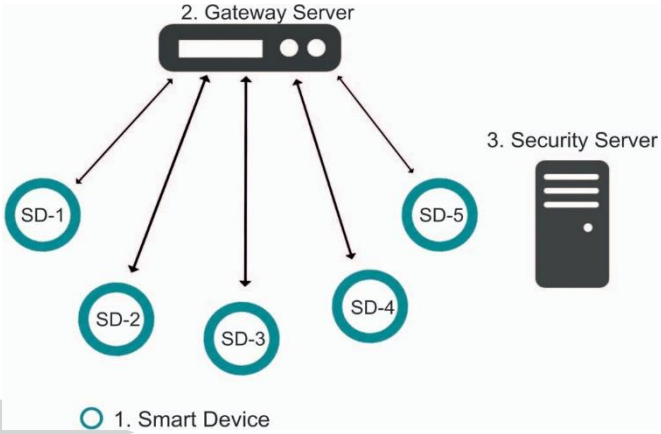

Fig. 1. Smart Home System Environment.

As shown in Fig.1, resource constrained smart devices (SD) communicate with Gateway Server (GS) over a wireless channel (e.g.,Zigbee, WiFi) [21] [3] [5]. The GS communicates with the resource constrained smart devices and controls them by providing instruction wirelessly. The SDs capture data through the connected sensors and sends the data wirelessly to Gateway Server where the data is analyzed and instructions to be per- formed are provided.

Fig.1 shows three main entities of SHS, given as follows:

1) SD sends home data to GS through the wireless link.
2) GS controls and manages all SDs. GS is incorporated with two interfaces:
   i. One for communicating with SDs,
   ii. Other is connected to the outside world through internet for providing data to the home users [20].
3) Security Server to generate and assign keys to the entities of smart home system.

B. Security Properties

Some works [17] [12] have identified several security properties for consideration in SHS from beginning. They are listed and explained as follows:

1) Mutual authentication: The adversary in smart home may pretend to be a legal entity by obtaining sensitive data from SD's or GS. Thus, mutual authentication and verification is important for the involved entities, thus prohibiting adversaries or compromised devices form

 DOI : 10.35291/2454-9150.2022.0468

getting unauthorized network access.

2) Session key establishment: Post verification, entities must agree on a session key to ensure security for inter-entity communication.

3) Message confidentiality: An adversary may eaves-drop, on a wireless channel, on the information transmitted between entities. Protocols are vulnerable to information leakage attacks. A basic approach here is protecting entity's data to maintain message confidentiality.

4) Message integrity: Message integrity ensures that messages sent be the sending entity is received by the receiving entity without modifications.

5) Lightweight-ness: Security protocols become an overhead for applications, thus we require lightweight session key establishment and authentication mechanism specially for resource con- strained SDs.

6) Safeguarding to well-known attacks: Proposed security scheme should be preventive to various popular and well-known attacks like masquerade, message forgery, known key, message replay and denial-of-service.

IV. PROPOSED SCHEME

For providing an adequate amount of security in SHS, this section proposes a scheme which fulfils the requirements for all security properties illustrated in Subsection III-B. Before participation, the smart devices require authentication in SHS. Our scheme can be applied in many different CPS applications, e.g., appliance control system, light system, climate control system, home care, etc. Table I shows the symbols used and our assumptions are as follows:

1) The Security Server (SS) and Gateway Server (GS) are connected and are secure entities of our system.

GS is tampered proof and is capable of protecting private data.

2) The symmetric key and hashing algorithms in GS and SDs are identical.

Symbols	Descriptions
SS	Security Server
AK_A	Authentication key for SD A
EK_A	Encryption Key for SD A
GI_A	Gateway Server Identifier for SD A
E_A[m]	Encrypts message m for SD A.
D_A[m]	Decrypts message m for SD A.
$HMAC$	Hashed Machine Authentication Code
$h()$	Hash function
$\|\|$	Concatenation operation

TABLE I: SYMBOLS AND DESCRIPTIONS

Our proposed scheme includes two phases:

1) System Initialization Phase.

2) Authentication and Session Key Establishment Phase.

A. System Initialization

Initially, all the system entities have to register themselves with the Security Server (SS) through an offline process and obtain security parameters. Before the deployment of devices in the network, for every smart device (SD) A, the SS generates and assigns a unique encryption key (EK_A), a unique authentication key (AK_A) and a unique gateway identifier (GI_A). Along with this, EK_A, AK_A, GI_A is also stored in GS. SS is responsible for maintaining all the databases. For security purposes, all the security keys are assigned a lifetime, which totally depends in the SS.

B. Authentication and Session Key Establishment Phase

For maintaining the initial trust among SDs, we present an authentication and key establishment mechanism, which is presented in four steps as follows:

Step1: Performed by Smart Device A.

1) Generate random nonce s and store it.

2) Generate random number r1.

3) Calculate authentication token,

$AT_A = h (GI_A || AK_A || r1)$.

4) Calculate session token,

$ST_A = E_A (AK_A, s, r1)$ encrypting using key EK_A.

5) Calculate tag1A = HMAC (AT_A, GI_A || s).

6) Send $tag1_A$, ST_A to SD_A.

Step2: Performed by Gateway Server for SD A.

1) Receive {$tag1_A$, ST_A} from SD_A.

2) Decrypt session token, ST_A with key EK_A and extract

{AT_A, s, r1}.

3) Check if s exists; if true then exit else store s.

4) Calculate authentication token,

$AT'_A = h (GI_A || AK_A || r1)$.

5) Check $AT_A = = AT_A$, if true then proceed else exit.

6) Calculate $tag1'_A$ = HMAC (AT_A, GI_A ||s).

7) Check $tag1'_A = = tag1_A$; if true then proceed else exit.

8) Generate random number r2.

9) Calculate session key, $SK_A = h (GI_A || s || AT_A)$.

 DOI : 10.35291/2454-9150.2022.0468

10) Calculate $tag2_A = E_A (SK_A, s, r2)$.

11) Send $\{tag2_A, r2\}$ to smart device SD_A.

12) Use SK_A as a session key.

Step3: Performed by Smart Device A.

1) Receive $\{tag2_A, r2\}$ from GS.

2) Decrypt $tag2_A$ with key KE_A and extract $\{SK_A, s, r2'\}$.

3) Check if received s == sent s; if true then proceed

else exit.

4) Check r2 == r2'; if true then proceed else exit.

5) Calculate session key, $SK'_A = h (GIA \|s \| AT_A)$.

6) Check $SK'_A == SK_A$; if true then proceed else exit.

7) Use SK_A as the session key.

V. EVALUATION

This section shows the evaluation of the proposed scheme using proof-of-concept scenario.

A. **Preposition**: Resilience to masquerade attacks.

Proof: Masquerading as a legal entity between the gateway server and the smart device A for joining the smart home network cannot be done.

Scenario: Consider an adversary X that captures the request message $\{tag1_A, ST_A\}$ sent from SD-A to GS and initiates a masquerading attack to join the GS by sending a fake request $\{tag1_X, ST_X\}$ to the GS. Adversary X computes $tag1_X = HMAC (AT_X, GI_X\| s_X)$ and

$AT_X = h (GI_X \| AK_X\| r1_X)$.

Resilience: The gateway identifier GI_A and authentication key AK_A is hidden; thus, the GS cannot verify fake identity sent by adversary X using AT_X and $tag1_X$. In order to generate the same HMAC, the adversary X need to compute the authentication token (AT_A) of device A, but in order to compute AT_A, the adversary X requires the real GI_A and AK_A values which are hidden. Hence

adversary X cannot be authenticated at GS due to the use of garbled keys GI_X and AK_X by the adversary X.

A. **Preposition:** *Resilience to replay attacks.*

Proof: On intercepting the message sent from the smart device to the GS and replaying the message to the GS, the GS rejects the replayed message.

Scenario: Consider an adversary X that captures the request message $\{tag1_A, ST_A\}$ sent from SD-A to GS and replays the message after certain intervals of time. Resilience: The SD generates the random nonce s and stores it. The generated random nonce s is sent in encrypted format to the GS. GS keeps the copy of the received nonce as described in Step2 of Section IV. Hence, in a replay packet, as the received nonce is already known to the GS, it rejects the replayed message.

V. CONCLUSION

It observed that the trend for having smart home environments is almost under its way like connected homes, in-house climate control system, intelligent light systems, security and safety systems. The security issues, challenges and observations related to CPS system explained by the many researchers It is also worth noting that the elderly population is increasing and adoption of smart home technology for elderly people is a major challenge. However, with a lot of good sides to SHE, if the services are exploited by an adversary, then it can cause disasters for the users. Thus, in this paper, we proposed a secure and light session key establishment algorithm considering the resource constrained smart devices for smart home environments. The evaluation of the proposed scheme demonstrated resilience of the proposed scheme against masquerading and replay attacks.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers, that helped to improve the quality of the manuscript.

REFERENCES

[1] Hope-smart home for elderly people [online]. *Available: http://www.hope-project.eu/.*

[2] Sm4all - smart homes for all [online]. *Available: http://www.sm4all-project.eu/.*

[3] E. Ayday and S. Rajagopal. Secure device authentication mechanisms for the smart grid-enabled home area networks. *pp. 1-18*, 2013.

[4] M. Burrough and J. Gill. Smart thermostat security: Turning up the heat [online]. *Available: http://www.burrough.org/Documents/Thermostat-final- paper.pdf.*

[5] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl. Home networking with ieee 802.15.4: a developing standard for low-rate wireless personal area net- works. *IEEE Communications Magazine*, 40(8):70–77, Aug 2002.

[6] Y. Chen and B. Luo. S2a: Secure smart household appliances. *Proceedings of the Second ACM Conference on Data and Application Security and Privacy, ser. CODASPY 12, pp. 217- 228*, 2012.

[7] X. Dong, K. Patil, J. Mao, and Z. Liang. A comprehensive client-side behavior model for diagnosing attacks in ajax applications. In *Engineering of Complex Computer Systems (ICECCS), 2013 18th International Conference on*, pages 177– 187, July 2013.

 DOI : 10.35291/2454-9150.2022.0468

[8] B. Fabian and T. Feldhaus. Privacy-preserving data infras- tructure for smart home appliances based on the octopus dht. *Computers in Industry, vol. 65, no. 8, pp. 1147 - 1160*, 2014.

[9] C. Gomez and J. Paradells. Wireless home automation net- works: A survey of architectures and technologies. *IEEE Communications Magazine*, 48(6):92–101, June 2010.

[10] S. Guillet, B. Bouchard, and A. Bouzouane. Correct by construction security approach to design fault tolerant smart homes for disabled people. *Procedia Computer Science, vol. 21, no. 0, pp. 257 - 264*, 2013.

[11] K. Han, J. Kim, T. Shon, and D. Ko. A novel secure key paring protocol for rf4ce ubiquitous smart home systems. *Personal and Ubiquitous Computing, vol. 17, no. 5, pp. 945-949*, June 2013.

[12] K. Islam, W. Shen, and X. Wang. Security and privacy considerations for wireless sensor networks in smart home environments. In *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference*, pages 626–633, May 2012.

[13] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse. Seamless integration of heterogeneous devices and access control in smart homes. In *Intelligent Environments (IE), 2012 8th International Conference*, pages 206–213, June 2012.

[14] N. Komninos, E. Philippou, and A. Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys Tutorials*, 16(4):1933–1954, Fourthquarter 2014.

[15] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sensors Journal*, 16(1):254– 264, Jan 2016.

[16] Y. Li. Design of a key establishment protocol for smart home energy management system. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference*, pages 88–93, June 2013.

[17] M.Georgios, L.Dimitrios, and K.Nikos. Security in smart home environment. *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications, IGI global*, 2006.

[18] K. Patil, X. Dong, X. Li, Z. Liang, and X. Jiang. Towards fine- grained access control in javascript contexts. In *Distributed Computing Systems (ICDCS), 2011 31st International Confer- ence on*, pages 720–729, June 2011.

[19] K. Patil and B. Frederik. A measurement study of the content security policy on real-world applications. *International Journal of Network Security*, 18(2):383–392, March 2016.

[20] H. Tschofenig and J. Arkko. Report from the smart object workshop. *Internet Draft, Internet Engineering Task Force*, April 2012.

[21] H. Tschofenig, J. Arkko, and D. McPherson. Architectural considerations in smart object networking. *Internet Draft, Internet Engineering Task Force*, July 2014.

[22] B. Vaidya, D. Makrakis, and H. T. Mouftah. Device au- thentication mechanism for smart energy home area networks. In *Consumer Electronics (ICCE), 2011 IEEE International Conference*, pages 787–788, Jan 2011.

[23] Wang, E. K., Ye, Y. and Xu, X. (2010) 'Security Issues and Challenges for Cyber Physical System'. doi: 10.1109/GreenCom-CPSCom.2010.36.

[24] Ashibani, Y. and Mahmoud, Qusay H (2017) 'Cyber physical systems security: Analysis, challenges and solutions', *Computers & Security*, 68, pp. 81–97. doi: 10.1016/j.cose.2017.04.005

[25] Wurm, J. *et al.* (2017) 'Introduction to Cyber-Physical System Security: A Cross-Layer Perspective', *IEEE Transactions on Multi-Scale Computing Systems*, 3(3), pp.215–227.doi: 10.1109/TMSCS.2016.2569446.

[26] Kim, B., Yoon, S., Kang, Y. and Choi, D. (2020). Secure IoT Device Authentication Scheme using Key Hiding Technology. 2020 International Conference on Information and Communication Technology Convergence (ICTC).

 DOI : 10.35291/2454-9150.2022.0468